## PESC61

## Security Protocol Processor PCI Express Server Adapter / CN1610 Cavium® Based

### Product Description

The Silicom protocol processor adapter is a complete PCI Express server adapter solution that incorporates IPSec, IKE, SSL and TLS protocol processing. The Silicom protocol processor PCI Express adapter is based on the Cavium Nitrox PX Security macro processor.

The Silicom protocol processor PCI Express adapter provides bulk cryptographic acceleration for 3DES, DES, AES and ARCFOUR symmetric encryption algorithms, for the SHA-1 and MD5 hash algorithm, and for the HMAC-SHA-1 and HMAC-MD5 keyed authentication algorithms. It provides public key acceleration for the RSA, DSA, and diffie-Helman asymmetric algorithms, as well as basic Modular Math functions.

The Silicom protocol processor PCI Express adapter provides a True Random Number Generator and can use it to generate on-chip random values for Diffie-Helman key generation and DSA signatures. The Silicom protocol processor PCI Express adapter provides combined encryption and HMAC authentication for single authentication for single-pass IPSec processing. It also executes protocol-specific instruction to support the SSL/TLS or IPSec/IKE security protocols.

Macro processing within the CN1610 processor, allows systems to offload high-level SSL or IPSec protocol commands that reduce the host I/O traffic and system processor to increase the total system throughput. This also frees system processor resources for other functions, increasing overall system performance.

The Silicom Protocol Processor PCI Express adapter is the ideal solution for high-end and mid-end virtual private networking (VPN), firewall appliances and SSL-based appliances.

### Key Features

- Single Chip solutions that accelerates all cryptographic operations and the SSL, IPSec / IKE, and CCMP protocols

- Up to 16K 180-bit Diffie-Hellman Public Key generation (groups 1,2,5)

- Up to 8K 1024-bit RSA operations/second

- Up to 1.0Gbps Bulk Data Encryption + Hashing (SSL, IPSec, or CCMP)

- Multi Algorithm support

- RSA and Diffie-Helman (Groups 1,2,5)

- DES/3DES, AES, ARCFOUR

- MD5, SHA-1, HMAC-MD5, HMAC-SHA-1

- AES-GCM

- KASUMI

- SHA-256/384/512

- 200Mbps Random Number Generator

**Host Interface:**

- PCI Express x4 lanes

**Applications:**

- VPN appliances

- VPN firewalls, routers and switches

- Secure WEB Servers and storage

- Secure Access devices

## Technical Specifications

| System Throughout | |
|---|---|
| System Throughout values are shown below. System values represent measured, memory-to-memory, in-system throughout on an optional platform using large buffer sizes and maximum pipelining | |
| **Function** | **Value** |
| **Full SSL processing throughout AES+SHA** | 1000 Mbp/s |
| **Full IPSec AES/SHA** | 1000 Mbp/s |
| **MAX Diffie-Helman (1024-bit module, 180-bit exponent)** | 1600 Transaction /Second |
| **MAX RSA 1024-bit exponent with CRT** | 8000Transaction /Second |
| **Random Number Generator** | 200 Mbps |
| **Operating Systems Support** | |
| **Operating system support:** | Linux FreeBSD |

| General Technical Specifications | |
| --- | --- |
| **Interface Standard:** | PCI Express Base Specification Revision 1.0 |
| **Board Size:** | Low profile short add in Card 127.0 mm x 68.9mm (5.0"x2.71") |
| **PCI Express Card Type:** | X4 Lane |
| **PCI Express Voltage:** | +3.3V +-9% |
| **PCI Connector:** | X4 Lane |
| **Controller:** | Cavium CN1610 |
| **Holder:** | Metal Bracket |
| **Operating Temperature:** | 0°C – 50°C (32°F – 122°F) |
| **Storage:** | -20°C–65°C (-4°F–149°F) |
| **EMC Certifications:** | FCC Part 15, Subpart B Class B<br>Conducted Emissions<br>Radiated Emissions<br>CE EN 55022: 1998 Class B Amendments A1: 2000; A2: 2003<br>Conducted Emissions<br>Radiated Emissions<br>CE EN 55024: 1998 Amendments A1: 2000; A2: 2003<br>Immunity for ITE Amendment A1: 2001<br>CE EN 61000-3-2 2000, Class A<br>Harmonic Current Emissions<br>CE EN 61000 3-3 1995, Amendment A1: 2001<br>Voltage Fluctuations and Flicker<br>CE IEC 6100-4-2: 1995<br>ESD Air Discharge 8kV. Contact Discharge 4kV.<br>CE IEC 6100-4-3:1995<br>Radiated Immunity (80-1000Mhz), 3V/m 80% A.M. by 1kHz<br>CE IEC 6100-4-4:1995<br>EFT/B: Immunity to electrical fast transients 1kV Power<br>Leads, 0.5Kv Signals Leads<br>CE IEC 6100-4-5:1995<br>Immunity to conductive surges COM Mode; 2kV,<br>Dif. Mode 1kV<br>CE IEC 6100-4-6:1996<br>Conducted immunity (0.15-80 MHz) 3VRMS 80% A.M. |

| | By 1kHz |
| --- | --- |
| | CE IEC 6100-4-11:1994 |
| | Voltage Dips and Short Interruptions |
| | V reduc >95%, 30% >95% Duration 0.5per, 25per, 250per |

## Order Information

| P/N | Description | Notes |
| --- | --- | --- |
| **PESC61-RoHS** | Security Protocol Processor PCI Express Adapter / CN1610 | Low profile Adapter, X4 |

Note: Model P/N -LP /-RoHS

-RoHS: RoHS Compliant / Lead free adapter.

-LP: Assemble Low Profile Metal Bracket

**1V0**